

**System and Method for Multiple Users to  
Securely Access Encrypted Data on a Computer System**

**ABSTRACT**

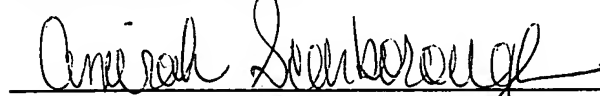
5 A method and system for encrypting non-volatile  
storage regions, such as volumes, accessible by multiple  
users. A plurality of non-volatile storage regions is  
encrypted each with a different encryption key. A subset  
of the encryption keys is made available to each user  
thereby granting the user access to a corresponding subset  
10 of non-volatile storage regions. To protect a user's  
encryption keys, a private-public encryption key pair is  
generated, the private key being made available only to  
that user. The subset of the user's encryption keys is  
encrypted using the user's public encryption key. The  
15 users' private keys can be stored in a secure encryption  
module and can be protected with a password. Upon  
authenticating a user, the corresponding encryption keys  
may be provided to the user after decrypting the encryption  
keys using the user's private key. The contents of the  
20 non-volatile storage regions are then decrypted using the  
encryption keys.

**CERTIFICATE OF MAILING UNDER 37 CFR§ 1.10**

I hereby certify that this correspondence is being deposited with the  
United States Postal Service as Express Mail in an envelope addressed to  
the Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450  
on

11-21-2005

EXPRESS MAIL LABEL: EV331727613US

  
Signature of Person Mailing Documents